AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 30 (Canceled).

31. (New) A method for using digital signatures to validate an amendment to a financial transaction, comprising:

receiving a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a representative of the first party and includes a suggested change to at least one term of the financial transaction;

validating that the representative of the first party has permission to make the amendment to the financial transaction by using a public key of a security officer associated with the first party to verify that the permission information was signed by a corresponding private key belonging to the security officer associated with the first party, thereby authorizing the representative of the first party to make the amendment;

validating that the representative of the first party digitally signed the request by using a public key of the representative of the first party to verify that the request was signed by a corresponding private key belonging to the representative of the first party;

when the validation establishes that the representative of the first party signed the request, and when the second party desires to agree to the request, allowing a representative of the second party to confirm the request by digitally signing the request with a private key belonging to the representative of the second party, and

returning the confirmed request to the first party;

wherein the representative of the first party and the security officer associated with the first party are separate entities; whereby requiring signatures from both the representative of the first party and the security officer associated with the first party prevents perpetration of fraud by a single entity.

32. (New) The method of claim 31, further comprising, when the validation establishes that the representative of the first party signed the request, and when the second party does not agree to the request but instead desires to propose counter-terms, allowing the second party to propose counter-terms by:

creating a responding request including a responding amendment with the counter-terms;

allowing the representative of the second party to digitally sign the responding request with a private key belonging to the representative of the second party; and

sending the signed responding request to the first party.

33. (New) The method of claim 32, further comprising:

validating that the representative of the second party digitally signed the responding request by using a public key of the representative of the second party to verify that the responding request was signed by a corresponding private key belonging to the representative of the second party; and

when the validation establishes that the representative of the second party signed the responding request, and when the first party desires to agree to the responding request, allowing the representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the representative of the first party, and

returning the confirmed responding request to the second party.

34. (New) The method of claim 33, further comprising, prior to allowing the representative of the first party to confirm the responding request, validating that the representative of the second party has permission to agree to the amendment by verifying that permission information for the representative of the second party is digitally signed by a security officer associated with the second party.

35. (New) The method of claim 31, further comprising recording the request and any response to the request in a database.

36. (New) The method of claim 31, further comprising validating an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

37. (New) The method of claim 31,

wherein receiving the request from the first party involves receiving the request from a trade facilitator that previously received the request from the first party; and wherein returning the confirmed request to the first party involves forwarding the confirmed request to the first party through the trade facilitator.

38. (New) The method of claim 31, wherein prior to receiving the request to make the amendment, the method further comprises, allowing the representative of the first party to obtain permission to amend the financial transaction by:

sending a request for permission to the security officer associated with the first party; and

allowing the security officer associated with the first party to digitally sign a permission record to indicate the representative of the first party has permission to agree to the amendment.

39. (New) The method of claim 31, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.

40. (New) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for

using digital signatures to validate an amendment to a financial transaction, the method comprising:

receiving a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a representative of the first party and includes a suggested change to at least one term of the financial transaction;

validating that the representative of the first party has permission to make the amendment to the financial transaction by using a public key of a security officer associated with the first party to verify that the permission information was signed by a corresponding private key belonging to the security officer associated with the first party, thereby authorizing the representative of the first party to make the amendment;

validating that the representative of the first party digitally signed the request by using a public key of the first to verify that the request was signed by a corresponding private key belonging to the first representative of the first party;

when the validation establishes that the representative signed the request and when the second party desires to agree to the request,

allowing a representative of the second party to confirm the request by digitally signing the request with a private key belonging to the representative of the second party, and

returning the confirmed request to the first party

wherein the representative of the first party and the security officer associated with the first party are separate entities; whereby requiring signatures from both the representative of the first party and the security officer associated with the first party prevents perpetration of fraud by a single entity.

41. (New) The computer-readable storage medium of claim 40, wherein when the validation establishes that the representative of the first party signed the request, and when the second party does not agree to the request, but instead desires to propose counter-terms, the method further comprises allowing the second party to propose counter-terms by:

creating a responding request including a responding amendment with the counter-terms;

allowing the representative of the second party to digitally sign the responding request with a private key belonging to the representative of the second party; and

sending the signed responding request to the first party.

42. (New) The computer-readable storage medium of claim 40, wherein the method further comprises:

validating that the representative of the second party digitally signed the responding request by using a public key of the representative of the second party to verify that the responding request was signed by a corresponding private key belonging to the representative of the second party; and

when the validation establishes that the representative of the second party signed the responding request, and when the first party desires to agree to the responding request,

allowing the representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the representative of the first party, and

returning the confirmed responding request to the second party.

43. (New) The computer-readable storage medium of claim 42, wherein prior to allowing the representative of the first party to confirm the responding request, the method further comprises validating that the representative of the second party has permission to agree to the amendment by verifying that permission information for the representative of the second party is digitally signed by a security officer associated with the second party.

44. (New) The computer-readable storage medium of claim 40, wherein the method further comprises recording the request and any response to the request in a database.

45. (New) The computer-readable storage medium of claim 40, wherein the method further comprises validating an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

46. (New) The computer-readable storage medium of claim 40,

wherein receiving the request from the first party involves receiving the request from a trade facilitator that previously received the request from the first party; and

wherein returning the confirmed request to the first party involves forwarding the confirmed request to the first party through the trade facilitator.

47. (New) The computer-readable storage medium of claim 40, wherein prior to receiving the request to make the amendment, the method further

comprises allowing the representative of the first party to obtain permission to amend the financial transaction by:

sending a request for permission to the security officer associated with the first party; and

allowing the security officer associated with the first party to digitally sign a permission record to indicate the representative of the first party has permission to agree to the amendment.

48. (New) The computer-readable storage medium of claim 40, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.

49. (New) An apparatus that uses digital signatures to validate an amendment to a financial transaction, comprising:

a receiving mechanism that is configured to receive a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a representative of the first party and includes a suggested change to at least one term of the financial transaction;

a validation mechanism that is configured to validate that the representative of the first party digitally signed the request by using a public key of the representative of the first party to verify that the request was signed by a corresponding private key belonging to the representative of the first party;

the validation mechanism further configured to validate that the representative of the first party has permission to make the amendment to the financial transaction by using a public key of a security officer associated with the first party to verify that the permission information was signed by a corresponding private key belonging to the security officer associated with the first party, thereby authorizing the representative of the first party to make the amendment;

an agreement mechanism, wherein when the validation establishes that the representative of the first party signed the request, and when the second party desires to agree to the request, the agreement mechanism is configured to,

allow a representative of the second party to confirm the request by digitally signing the request with a private key belonging to the representative of the second party, and to

return the confirmed request to the first party

wherein the representative of the first party and the security officer associated with the first party are separate entities; whereby requiring signatures from both the representative of the first party and the security officer associated with the first party prevents perpetration of fraud by a single entity.

50. (New) The apparatus of claim 49, wherein when the validation establishes that the representative of the first party signed the request, and when the second party does not agree to the request, but instead desires to propose counter-terms, the agreement mechanism is configured to:

create a responding request including a responding amendment with the counter-terms;

allow the representative of the second party to digitally sign the responding request with a private key belonging to the representative of the second party; and to

send the signed responding request to the first party.

51. (New) The apparatus of claim 50, further comprising:

a second validation mechanism associated with the first party;

wherein the second validation mechanism is configured to validate that the representative of the second party digitally signed the responding request by using a public key of the representative of the second party to verify that the responding request was signed by a corresponding private key belonging to the representative of the second party; and

a second agreement mechanism associated with the first party;

wherein when the validation establishes that the representative of the second party signed the responding request, and when the first party desires to agree to the responding request, the second agreement mechanism is configured to,

allow the representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the representative of the first party, and to

return the confirmed responding request to the second party.

52. (New) The apparatus of claim 51, wherein prior to allowing the representative of the first party to confirm the responding request, the second validation mechanism is configured to validate that the representative of the second party has permission to agree to the amendment by verifying that

permission information for the representative of the second party is digitally signed by a security officer associated with the second party.

53. (New) The apparatus of claim 49, further comprising an archiving mechanism that is configured to record the request and any response to the request in a database.

54. (New) The apparatus of claim 49, wherein the validation mechanism is configured to validate an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

55. (New) The apparatus of claim 49,

wherein the receiving mechanism is configured to receive the request from a trade facilitator that previously received the request from the first party; and

wherein the agreement mechanism is configured to return the confirmed request to the first party by forwarding the confirmed request to the first party through the trade facilitator.

56. (New) The apparatus of claim 49, further comprising a permission obtaining mechanism, wherein prior to receiving the request to make the amendment, the permission obtaining mechanism is configured to:

send a request for permission to the security officer associated with the first party; and to allow the security officer associated with the first party to digitally sign a permission record to indicate the representative of the first party has permission to agree to the amendment.

57. (New) The apparatus of claim 49, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.